Data Attacks and Security Techniques in Mobile Computing

G.V.Vijey Kaarthic, M. Mohammed Arfath & R.Divya

ABSTRACT

Mobile computing is the availability of cloud computing services in a mobile environment. By providing optimal services for mobile users incorporates the elements of mobile networks and cloud computing. Mobile computing is human–computer interaction by which a computer is expected to be transported during normal usage, which allows for transmission of data, voice and video. Communication issues include ad hoc networks and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. Hardware includes mobile devices or device components. Mobile software deals with the characteristics and requirements of mobile applications. Network security consists of the policies and practices adopted to prevent and monitor unauthorized access, misuse, modification, or denial of a computer network and network-accessible resources. Network security involves the authorization of access to data in a network, which is controlled by the network administrator.

Keywords: Mobile Computing, Security Attacks, Security Issues, Security Techniques

1. INTRODUCTION

Mobility refers to portability or possibility of moving to different locations and across multiple times using different types of mobile devices. The internet and mobile technologies have increased the popularity of mobile application in modern society. Mobile application refers to any software applications that run using mobile devices [2]. Computer security, also known as cyber security or IT security, is the protection of computer systems from the theft or damage to the hardware, software or the information on them, as well as from disruption or misdirection of the services they provide. It includes controlling physical access to the hardware, as well as protecting against harm that may come via network access, data and code injection,[2] and due to malpractice by operators, whether intentional, accidental, or due to them being tricked into deviating from secure procedures.[3] The field is of growing importance due to the increasing reliance on computer systems and the Internet in most societies,[4] wireless networks such as Bluetooth and Wi-Fi – and the growth of "smart" devices, including smart phones, televisions and tiny devices as part of the Internet of Things. Denial of service attacks (DoS) are designed to make a machine or network resource unavailable to its intended users.[6] Attackers can deny service to individual victims, such as by deliberately entering a wrong password enough consecutive times to cause the victim account to be locked, or they may overload the capabilities of a machine or network and block all users at once. While a network attack from a single IP address can be blocked by adding a new firewall rule, many forms of Distributed denial of service (DDoS) attacks are possible, where the attack comes from a large number of points – and defending is much more difficult.

G.V.Vijey Kaarthic, Assistant Professor, Department of Master of Applications(MCA),Er.Perumal Manimekalai College of Engineering,Hosur,Tamil Nadu.

M. Mohammed Arfath, Second Year MCA, Er.Perumal Manimekalai College of Engineering,Hosur, ,Tamil Nadu.

R.Divya, Second Year MCA, Er.Perumal Manimekalai College of Engineering,Hosur,Tamil Nadu.

2. MOBILE COMPUTING

Mobile computing is human–computer interaction by which a computer is expected to be transported during normal usage, which allows for transmission of data, voice and video. Mobile computing involves mobile communication, mobile hardware, and mobile software. Communication issues include ad hoc networks and infrastructure networks as well as communication properties, protocols, data formats and concrete technologies. Hardware includes mobile devices or device components. Mobile software deals with the characteristics and requirements of mobile applications. The main architecture of MCC is composed from the components: mobile users, mobile operators, internet service providers (ISP), cloud service providers, respectively.

Mobile computing devices include

- Laptops
- PDAs and handheld PC
- Smart and mobile phones
- Pagers

3. LITERATURE REVIEW

Though still now it is on the early stage of development, in future mobile cloud computing could become the major model for mobile application[2]. According to a recent research, more than 240 million businesses will use cloud services through mobile devices by 2015 and will push the revenue of mobile computing to $5.2 billion [7]. With this major importance, this paper has provided an overview of mobile computing in which its definitions, architecture, and advantages have been presented [3]. As the mobile devices have certain resource constraints, there arises a need to get resources from external sources. One of the ways to overcome this problem is getting resources from a cloud, but the access to such platforms is not always guaranteed or/and is too expensive. Future work includes a systematic definition of different security policies that are used by different backbone networks [5]. By providing optimal services for mobile users MCC incorporates the elements of mobile networks and cloud computing [4].

4. MOBILE SECURITY

Mobile security or mobile phone security has become increasingly important in mobile computing. Of particular concern is the security of personal and business information now stored on Smartphone.

More and more users and businesses use Smartphone to communicate, but also to plan and organize their users' work and also private life. Within companies, these technologies are causing profound changes in the organization of information systems and therefore they have become the source of new risks. Indeed, smartphones collect and compile an increasing amount of sensitive information to which access must be controlled to protect the privacy of the user and the intellectual property of the company.

All Smartphone, as computers, are preferred targets of attacks. These attacks exploit weaknesses inherent in Smartphone that can come from the communication mode—like Short Message Service (SMS, aka text messaging), Multimedia Messaging Service (MMS), wifi, Bluetooth and GSM, the *de facto* global standard for mobile communications. There are also exploits that target software vulnerabilities in the browser or operating system. And some malicious software relies on the weak knowledge of an average user.

Security counter-measures are being developed and applied to Smartphone, from security in different layers of software to the dissemination of information to end users. There are good practices to be observed at all levels, from design to use, through the development of operating systems, software layers, and downloadable apps.

In mobile cloud computing applications security and privacy are the key issues and still face some enormous challenges. Another big problem plaguing mobile computing is credential verification. As other users share username and passwords, it poses as a major threat to security. This being a very sensitive issue, most companies are very reluctant to implement mobile computing to the dangers of misrepresentation.

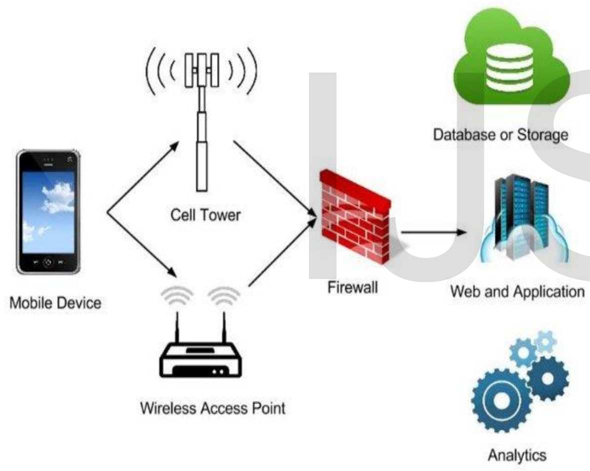

Fig 1: Mobile security [7]

5. SECURITY ATTACKS

"Mobile devices face an array of threats that take advantage of numerous vulnerabilities commonly found in such devices. These vulnerabilities can be the result of inadequate technical controls, but they can also result from the poor security practices of consumers," the GAO stated. "Private [companies] and relevant federal agencies have taken steps to improve the security of mobile devices, including making certain controls available for consumers to use if they wish and promulgating information about recommended mobile security practices.

5.1 Problems in security attacks

1. Sent by a mobile device is usually not encrypted while in transit.
2. Operating systems may be out-of-date. Security patches or fixes for mobile devices' operating systems are not always installed on mobile devices in a timely manner.
3. Mobile devices may Mobile devices often do not have passwords enabled. Mobile devices often lack passwords to authenticate users and control access to data stored on the devices.
4. Two-factor authentication is not always used when conducting sensitive transactions on mobile devices. According to studies, consumers generally use static passwords instead of two-factor authentication when conducting online sensitive transactions while using mobile devices.
5. Wireless transmissions are not always encrypted. Information such as e-mails have unauthorized modifications. The process of modifying a mobile device to remove its limitations so consumers can add features (known as "jail breaking" or "rooting") changes how security for the device is managed and could increase security risks.

5.2 Fight back of problems in security attacks

Enable user authentication: Devices can be configured to require passwords or PINs to gain access. In addition, the password field can be masked to prevent it from being observed, and the devices can activate idle-time screen locking to prevent unauthorized access.

Install a firewall: A personal firewall can protect against unauthorized connections by intercepting both incoming and outgoing connection attempts and blocking or permitting them based on a list of rules.

5.3 Mobile computing – security issues:

Security Issues in Mobile Computing. Securing information from unauthorized access is a major problem for any network - wire line or wireless Security, in a broad sense, focuses on network security, system security, information security, and physical security.

Data security and other security issues- mobile are famous for malicious code give possibility of loss

- Data loss from lost / stolen devices
- Info stealing by malicious malware
- Data leakage due to poorly written third party app

Un assured network access, unreliable APs

Insecure market places Near field communication and proximity based hacking

6. MOBILE COMPUTING IS LINK WITH OUR GOALS

Mobile computing is used for their technology programs to the members of joining in the mobile computing resources and work is more efficient and we can provide the small institution to achieve our goals. It achieve peoples very easily and then can have the very energetic.

In that now it technologies are supporting our mobile computing technologies for then some certain departments only for using programs developing otherwise finding new things about mobile device. Mobile computing is a developing resources to develop their works in the schools, colleges, and some organizations as well as the including the private sectors.

Now a days, students will about the mobile operating in an many ways. Because some social network applications are using all the peoples and learning some good and bad things and then some applications are using to develop their applications are using the networks. Some social networks are activating the mobile devices are inter activately of some relevant materials.

7. SECURITY MODES

Security modes refer to information systems security modes of operations used in mandatory access control (MAC) systems. Often, these systems contain information at various levels of security classification.

- Link –level security
- Service level security
- Bluetooth security

7.1 Link level security

Link level security refers to those security services that are invoked, directly or indirectly, by an MCA, the communications subsystem, or a combination of the two working together.

7.2 **Service level security**

Services running on a vanilla Linux system can give the cracker a host of information about your system that should otherwise not be available. Remember, the more information an intruder can gain about your system, the better chance they have at breaking in and doing some damage.

7.3 Bluetooth Security

Bluetooth allows different security levels to be defined for devices and services. Security levels has been used for the mobile device has unrestricted access to all some specific services (fig 2). That the device has been verified and trusted depended has confined access to administrations An automatic output power adaptation scheme is also included in the standard for the low power consumption of light weight mobile devices uses radio frequency waves will spread range for data transmission exactly according to requirements based on the detected intensity. Bluetooth is similar for the radio frequency waves for the technology to communicate the very short distance must download the information in the mobile or computers. Obtain this device connection through using the passwords to accept that sharing time process.

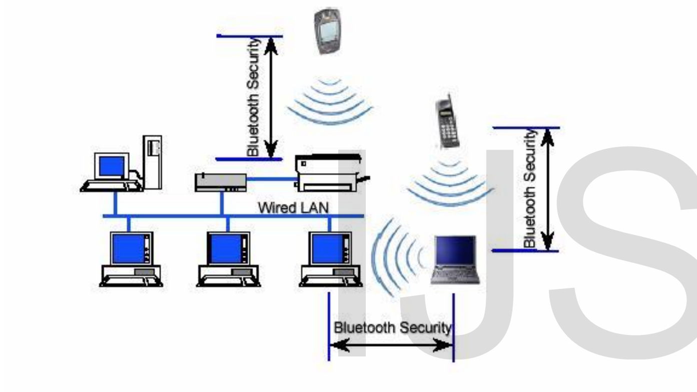

Fig 2: Bluetooth security[7]

8. SECURITY ATTACKS

In these security part is available the more risk wants secure the data safely and user passwords wants to keep them secretly. Some benefits from the Internet, networking is throughout the world and can gather information at any time in the mobiles, some them will hacks the passwords for the internet connection on your mobiles attacks may have the proper intention, such as theft the user names, passwords, credit card details, social security numbers, personal identification numbers and then others details can be used have the benefits and services.

- Passive attack
- Active attack

Files and programs of a network can be designated that you do not have to worry about illegal copying of programs. Username and passwords can be established for the specific directories to restrict access to authorized users for their personal details. Security is mainly using the big concern in wireless networking device and then especially in business m-commerce and e-commerce applications. Mobile users will increases the automatically security will concerns in wireless network connections. Current wireless networks employ authentication and data encryption techniques is interface to provide security to its users. The IEEE 801.11 standard wired equivalent privacy that will authenticates the users and to encrypt data between the PC and mobiles in the wireless LAN networks access points. In large enterprises of IP network level security solution could be ensured that the corporate network and proprietary data are safe.

8.1 Passive attack

A passive attack is a network attack in which a system is monitored and sometimes scanned for open ports and vulnerabilities. The purpose is solely to gain information about the target and no data is changed on the target. Passive attacks include active reconnaissance and passive reconnaissance.

8.2 Active attack

An active attack is a network exploit in which a hacker attempts to make changes to data on the target or data en route to the target. Types of active attacks: In a masquerade attack, the intruder pretends to be a particular user of a system to gain access or to gain greater privileges than they are authorized.

9. SECURITY TECHNIQUES

Security starts with authenticating, commonly with a username and a password. Since this requires just one detail authenticating the user name—i.e., the password—this is sometimes termed one-factor authentication. With two-factor authentication, something the user 'has' is also used (e.g., a security token or 'dongle', an ATM card, or a mobile phone); and with three-factor authentication, something the user 'is' is also used (e.g., a fingerprint or retinal scan). Major techniques in security that is encryption and decryption.

- Computer access control.
- Application security. Antivirus software. Secure coding. Security by design. Secure operating systems.
- Authentication. Multi-factor authentication.
- Authorization.
- Data-centric security.
- Firewall (computing)
- Intrusion detection system.
- Intrusion prevention system.

9.1 Biometric security devices

Upcoming days is advanced systems has require the biometric authentication. For log in into the very sophisticated laptops or also can develop to the mobiles security systems. In this some advanced mobiles security purposes also using for face recognition system or the fingerprint scanning. Some of the biometric authentications include the

- Eye scan (Retina scan)
- Face Identification
- Voice taking
- Finger print (Thumb Impression)

3.1 FINGER PRINT[7]

3.2 EYE SCAN[7]

10. CONCLUSION

Mobile computing is an important, evolving technology. It enables mobile personnel to effectively communicate and interact with the fixed organizational information system while remaining unconstrained by physical location. Mobile computing offers significant benefits for organizations that choose to integrate the technology into their fixed organizational information system. Mobile computing is made possible by portable computer hardware, software, and communications systems that interact with a non-mobile organizational information system while away from the normal, fixed workplace. Mobile computing is a versatile and potentially strategic technology that improves information quality and accessibility, increases operational efficiency, and enhances management effectiveness. Mobile computing may be implemented using many combinations of hardware, software, and communications technologies. The technologies must be carefully selected and the applications designed to achieve the business.

REFERENCES

1. S M Shamim., Angona sarker ., ali newaz bahar., md. Atiqur rahman 2015**. A review on mobile computing** (IJCA 2015).
2. Sonika and Sangeetha Rani **, Threats and Security Issues in Mobile computing**(2014)
3. Pallavi D. Dudhe and Prof. P.L. Ramkate**, Mobile computing with wireless LAN and its modes Adhoc Network with challenges**(2014).
4. Mohammed Sarrab and Hadj Bourdoucen , **Mobile cloud computing: security issues and considerations**(2015).
5. C. Shravanthi and H S Guruprasad , **Mobile cloud computing as future for mobile applications**(2014).
6. S. Gopalakrishnan**, A Survey of wireless network security** (IJCSMC 2014).
7. http://www.tutorialspoint.com/mobile computing.